An Analysis: Complex Interdependence and the Chinese-United States Cyber Relationship

Robert Maxwell Morrison

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Master of Arts
In
Political Science

Committee Chair: Aaron Brantly
Priya Dixit
Eric Jardine

April 25, 2018
Blacksburg, Virginia

Keywords: Complex Interdependence, Cyberespionage, Cyberspace.
An Analysis: Complex Interdependence and the Chinese-United States Cyber Relationship

Robert Maxwell Morrison

Abstract (Academic)

The United States and the People’s Republic of China maintain a unique relationship due to the high levels of interdependence between the countries’ political, economic, military, and social functions. This association has been complicated in the past by Chinese industrial cyberespionage (CE) carried out against United States organizations and individuals in pursuit of economic advancement. This paper examines the nature of Chinese-American relations and determines whether its features adhere to Robert Keohane and Joseph Nye’s theory of complex interdependence in Power and Interdependence. Further, this paper also explores possible reasons for a decline in Chinese CE beginning in mid-2014 and what impact this could have on the two countries’ relations moving forward.
An Analysis: Complex Interdependence and the Chinese-United States Cyber Relationship

Robert Maxwell Morrison

Abstract (Public)

The purpose of this thesis is to examine whether the United States and China have become interdependent through political, economic, military, and social means. Additionally, China has historically spied on and stolen United States’ secrets electronically for their own benefit. This trend began to slow down in mid-2014 and I offer several possible explanations for why this might have happened. Lastly, I conclude by seeing how this decline in Chinese spying reflects on the interdependent relationship between China and the United States.
Dedication

I dedicate this paper to my father and mother, Marty and Julie, and to my sister, Alexandra. They have provided me with unwavering support and encouragement as I have progressed through my undergraduate and graduate programs at Virginia Tech. Their patience and dedication to my continuing education have provided me with the resources I have needed to succeed and enjoy all of my learning experiences. Lastly, I also dedicate this thesis to the men and women in the United States Military and Intelligence Community who work hard on behalf of their nation to protect United States’ interests in cyberspace.
Acknowledgments

This paper would not have been possible without the support of numerous individuals who have encouraged and shaped me along the way. First, I want to sincerely thank Dr. Aaron Brantly for agreeing to serve as my thesis committee chair and for his constant feedback and help in aiding me to develop and refine my thesis topic and argument. Dr. Brantly has demonstrated to me what it takes to complete a robust research project from start to finish and has also been extremely helpful in narrowing my career aspirations. Second, I want to thank Drs. Priya Dixit and Eric Jardine for their willingness to serve as members on my thesis committee. Both Drs. Dixit and Jardine have been very helpful in helping me to develop specific and concentrated lines of inquiry for my research and I also thoroughly enjoyed the time I got to spend as a student in their courses as well. Third, I want to thank a non-exhaustive list of friends in Brooke Boutwell, Ryan Butterfield, Alex Eckert, Ryan Hasegawa, and Vern Ferguson for their support during my thesis project and for helping me to maintain an appropriate school-life balance during my busy graduate study years. Lastly, I want to thank Dr. Scott Nelson, Ms. Karen Nicholson, and the other professors I studied under during my graduate education—your support and challenging thoughts have been invaluable in developing me as a young man and I am appreciative of the time and effort you have invested into my future.
Table of Contents

Acknowledgments -V
List of Figures -VII
Introduction -1
Literature Review -5
Complex Interdependence Analysis -20
Chinese Cyberespionage Analysis -49
Conclusions -65
Summary -69
Works Cited -73
List of Figures

Figure 1: China’s Cyber Apparatus -12
Figure 2: United States-Chinese Economic Connections -21
Figure 3: Chinese Mineral Extraction in Africa -38
Figure 4: Chinese Espionage Model -51
Figure 5: Active Chinese Network Intrusions -52
Figure 6: Chinese Late-Stage Investment -58
Introduction

This paper argues that China and the United States interact within the framework of a complex interdependent relationship as outlined by Robert Keohane and Joseph Nye in *Power and Interdependence*. Within this complex interdependent relationship, China and the United States share multiple channels of communication, an absence of a well-defined hierarchy of issues, and no direct conventional military conflict. While there are cyber incidents, these do not obviate the conditions of interdependence. China and the United States have been successful in establishing linkage strategies, with both states pushing often-complementary agendas inclusive of transnational, transgovernmental, and international organizations. Where these agendas are not complementary there is continued dialogue. At its core the relationship between China and the United States is defined by what Keohane and Nye identify are sensitivities and vulnerabilities to one another’s actions. The management of the sensitivities and vulnerabilities allows for the shaping of interstate interactions through activities short of war.

To understand the current strategic outlook of the United States national security establishment, it is useful to look at documents published by the Department of Defense. In mid-January 2018, United States Secretary of Defense James Mattis released an updated National Defense Strategy outlining the Department of Defense’s primary goals and concerns dealing with American national security. In this document, the Pentagon summarizes the strategic environment in which foreign policy now occurs, states the Department’s objectives, and discusses America’s new strategic approach to build a more lethal force, strengthen existing alliances and connect with new partners, and to reform the Department for greater performance
and affordability. Moreover, a significant change found in this National Defense Strategy compared to those of the last seventeen years resides in its identification of inter-state strategic competition as the greatest threat to American national security, not terrorism.

Below I examine the nature of the relationship between the People’s Republic of China and the United States regarding cyberspace and analyze whether actions taken therein adhere to Robert Keohane and Joseph Nye’s theory of complex interdependence. As the National Defense Strategy states, “China is leveraging military modernization, influence operations, and predatory economics to coerce neighboring countries to reorder the Indo-Pacific region to their advantage.” Further, “As China continues its economic and military ascendance, asserting power through an all-of-nation long-term strategy, it will continue to pursue a military modernization program that seeks Indo-Pacific regional hegemony in the near-term and displacement of the United States to achieve global preeminence in the future.” This project seeks to explain why China’s CE experienced a significant decline starting in 2014 in order to understand what China’s goals and motivations are and also to demonstrate the value of this project to International Relations theory to show how complex interdependence applies to the 21st-century cyber environment.

First, below the key concepts that will be used throughout the work are defined to establish a technical baseline before proceeding into an explanation of the framework of complex interdependence theory. Second, I outline and explain how China’s military cyber forces are organized to facilitate their espionage enterprise. Third, I discuss and analyze China’s cyber

2 Ibid, 2.
3 Ibid.
doctrines of informatization, their information warfare doctrine, and their practices of active offense and defense. Fourth, I critically scrutinize Chinese and American actions in the context of complex interdependence theory to discover whether such a relationship currently exists. Fifth, I propose and examine five different possible explanations for why Chinese CE declined in 2014. Sixth, I reiterate the major tenets of my argument and conclude by explaining possible areas of future research and state the implications of my findings for U.S. national security moving forward.

Definitions

Cyberspace is widely seen as the new fifth domain of conflict in addition to the land, sea, air, and space arenas of engagement. However, it differs from its counterparts for four reasons: it is man-made, military capabilities across the other domains are managed through the cyber domain, military and civilian components of cyberspace are often intertwined, and attribution of action in cyberspace can be difficult to assign. Cyberspace for the purposes of this paper is defined as “A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.” This definition encompasses both the technical and policy implications of the domain.

Second, to explore the nature of Chinese-United States interdependence, the timeline of Chinese CE against the United States will be examined. For the purposes of this project, cyber espionage means “the unauthorized extraction of information from a computer system or

---

5 As cited in Brantly, 4.
network.” More specifically, CE focuses on China’s practices of stealing corporate and industrial secrets from entities within the United States and from other countries abroad.

Third, I define cyberwar as “a systematic campaign of cyberattacks for political or related military ends.” Moreover, this concept can be further divided into two types of cyberwar, namely strategic and operational cyberwar. The former can be defined as an attack that “targets a country, notably its critical systems; it is largely undertaken to influence the target or to weaken its ability to resource combat,” while the latter “targets military systems; it is largely undertaken in conjunction with war or a kinetic…military operation to enhance the latter’s success.”

Fourth, in describing and explaining Chinese cyber doctrine, it is necessary to define what is meant by informatization and offensive and defensive cyber operations. Informatization is “a means to ensure sustained economic growth, enable China to compete globally in the information technology realm, and to ensure national security against domestic and international threats” and is China’s overarching cyber goal. Offensive cyber operations are “Activities that, through the use of cyberspace, actively gather information from computers, information systems, or networks, or manipulate, disrupt, deny, degrade, or destroy targeted computers, information systems, or networks” while defensive cyber operations contain “All defensive countermeasures

---

7 Ibid.
designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace.”

Fifth and finally, two core concepts of Keohane and Nye’s formulation of complex interdependence are sensitivity and vulnerability and the two can be distinguished as follows: “In terms of the cost of dependence, sensitivity means liability to costly effects imposed from outside before policies are altered to try to change the situation. Vulnerability can be defined as an actor’s liability to suffer costs imposed by external events even after policies have been altered.”

**Literature Review**

Robert Keohane and Joseph Nye formulated their theory of complex interdependence in the 1970s in response to what they saw as several shortcomings in the predominant realist thinking of the time. To correct for this, they set out to explain why certain countries enjoyed peaceful relationships with one another, and their conclusions were that where “there are reciprocal (although not necessarily symmetrical) costly effects of transactions, there is interdependence.”

To fully explain their theory, Keohane and Nye established three primary characteristics that must be present for complex interdependence to exist: multiple channels among societies, absence of hierarchy among issues, and a minor role played by military force. For the authors, multiple channels among societies can exist including “informal ties between governmental elites as well as formal foreign office arrangements; informal ties among nongovernmental

---

10 Ibid, 8.
12 Ibid, 8.
elites… and transnational organizations.”\(^{13}\) These differences constitute interstate relations, transgovernmental relations, and transnational relations respectively and are significant because they bring into question the assumption that states are the only unit and that states act cohesively. Regarding the absence of a hierarchy of issues, the primary implication for their critique of the realist school is that military policy is no longer the only overriding matter of importance to states. Instead, many “issues arise from what used to be considered domestic policy, and the distinction between domestic and foreign issues becomes blurred. These issues are considered in several government departments (not just foreign offices), and at several levels.”\(^{14}\) Finally, if the previous two conditions are met, complex interdependence will prevail if “Military force is not used by governments toward other governments within the region, or on the issues.”\(^{15}\)

In order for the above characteristics of complex interdependence to emerge, four political processes must exist: linkage strategies, agenda setting, transnational and transgovernmental relations, and the role of international organizations. According to Keohane and Nye, in a state of complex interdependence, linkages “by strong states will be more difficult to make since force will be ineffective. Linkages by weak states through international organizations will erode rather than reinforce hierarchy.”\(^{16}\) Moreover, agendas “will be affected by changes in the distribution of power resources within issue areas; the status of international regimes; changes in the importance of transnational actors; linkages from other issues and politicization as a result of rising sensitivity interdependence.”\(^{17}\)

\(^{13}\) Ibid, 20.
\(^{14}\) Ibid.
\(^{15}\) Ibid, 21.
\(^{16}\) Ibid, 31.
\(^{17}\) Ibid.
For transnational and transgovernmental relations, the “existence of multiple channels of contact leads us to expect limits beyond those normally found in domestic politics, on the ability of statesmen to calculate the manipulation of interdependence or follow a consistent strategy linkage. Statesmen must consider differential as well as aggregate effects of interdependence strategies and their likely implications for politicization and agenda control.”\(^{18}\) This differs from the realist school of thought because realists consider security as the primary objective of the state. Security as the primary consideration controls how any agenda is set between states. Any departure from this standard constitutes a major challenge to basic realist theoretical assumptions.

Finally, in a relationship of complex interdependence, “Organizations will set agendas, induce coalition-formation, and act as arenas for political action by weak states. Ability to choose the organizational forum for an issue and to mobilize votes will be an important political resource.”\(^{19}\) Again, this differs from classical realism because for realism, states exist in an anarchic, self-help world in which alliances lead to the preponderance of the security dilemma. With complex interdependence, coalition forming is an acceptable means to achieving peace.

To further develop their work, Keohane and Nye differentiate between power over others and power over outcomes. At the bottom line, they conclude that for “international regimes to govern situations of complex interdependence successfully they must be congruent with the interests of powerfully placed domestic groups within major states, as well as with the structure of power among states.”\(^{20}\) There are few formally relevant regimes in this case because the

\(^{18}\) Ibid, 28.
\(^{19}\) Ibid, 31.
\(^{20}\) Ibid, 193.
ability to transform the political environment domestically and internationally resides with just a handful of major powers, two of which are China and the United States.

To advocate for why complex interdependence is still a useful theory and not an antiquated product of the 1970s, Keohane and Nye identify three trends that seem to indicate that interdependence will continue into the future. First, the “multiplicity of goals and difficulty in arranging them hierarchically are results of the long-term development of the welfare state.” Second, the “development of multiple channels of contact reflects a long-term historical trend in the technology of communications and transportation.” Third and finally, the “change in the role of military force is related to trends in the destructiveness of military technology and patterns of social mobilization.”

On the last point, cyber poses an interesting question, as it is not necessarily violently destructive in and of itself. Instead, cyber attacks rely on the manipulation of physical devices to achieve violence or other aims as desired.

To exploit and leverage the above conditions for their own benefit, states need to exercise one of three types of leadership: to direct or command, to go first, or to induce. These three methods correspond respectively to hegemony, unilateralism, and multilateralism and the method employed will differ depending on the goals certain states identify for themselves. Each major power must decide which form of leadership it will exercise within its own realm of influence and such decisions impact the formulation of interdependence globally. One implication of Keohane and Nye’s discussion of leadership pertaining to cyberspace is that states are no longer the only actors capable of initiating change. Private organizations and other civil society groups are now often able to manipulate traditional power actors in order to achieve their goals. This is done through leading the way with development of technology and effectively leveraging the

21 Ibid, 194.
important role of private resources used in cyberspace in order to secure outcomes favorable to one’s own interests.

In the cyber context of this project, Keohane and Nye provide a very useful design of how the developing information age impacts interdependence. At the bottom line, the authors argue that “by drastically reducing the costs of transmitting information, the information revolution creates a new politics of credibility in which transparency will increasingly be a power asset.” Keohane and Nye also argue that with the increase in free information flowing across societies, one effect is that “states have lost much of their control over information about their own societies.” This does not mean that strategic information, like classified national security documents, should be widely distributed. Instead, it means that soft power will increasingly become more important for states seeking to monitor information flows.

Moreover, Keohane and Nye describe how the nature of information impacts interdependence based on what is being transmitted, so they describe three different kinds of information. First, free information is that which “actors are willing to acquire and send without financial compensation. The sender gets advantages from the receiver believing the information, and hence has incentives to produce it. Scientific information falls into this category. So do persuasive messages, such as those in which politicians specialize.” Second, commercial information is that which “actors are willing to acquire and send at a price…Creating commercial information before one’s competitors can—if there is an effective system to protect intellectual property rights—creates first-mover advantages and enormous profits.” Third and

\[22\] Ibid, 213.
\[23\] Ibid, 222.
\[24\] Ibid, 223.
\[26\] Ibid.
finally, strategic information is that which “confers the greatest advantage on actors only if their competitors do not possess it. One way to think of strategic information is that it constitutes asymmetrical knowledge of a competitor’s strategy so that the outcome of a game is altered.”27

Within the cyber relationship between China and the United States, commercial and strategic information hold the greatest significance, as this information created and possessed by the United States is highly desirable for China as it continues to try to modernize and close the information gap with more advanced Western countries. As such, CE was a main tool used to access this information and its decline holds interesting implications for the changing nature of interdependence between the two countries. Interdependence between China and the United States did not come about as a result of a spontaneous incident. Instead, it was fostered over decades as the two countries increasingly opened up toward one another. What CE does imply regarding complex interdependence is that United States’ actions starting mid-2014 showed that the U.S. was willing to alter the shadow of the future with China. If CE would no longer be tolerated because of its deleterious effects, the United States might have been willing to sever its interdependence with China in other ways. Additionally, the decline in CE also showed that the United States and China were sensitive and vulnerable to one another and U.S. actions to end the CE signaled this. While Keohane and Nye’s theoretical formulation is helpful in understanding the interdependent relationship between China and the United States, several other works also contribute useful literature to better understand this project’s fitting in the existing field.

To explain China’s cyber doctrine and organizational hierarchy, Jon Lindsay, Tai Ming Cheung, and Derek Reveron undertook a project to highlight an expansive and complex enterprise. Their work is helpful in developing components supporting this analysis through their

27 Ibid.
discussion of how China’s cyber organizations relate to one another and their descriptions of informatization. Specifically of interest is China’s information warfare doctrine, and active offense and defense concepts.

Figure 1 illustrates the organizational hierarchy of the Chinese cybersecurity apparatus. For the purposes of economic espionage, the primary actor is the People’s Liberation Army’s 3rd Department, which resides first under the Communist Party Politburo, then under the Military Commission, and then under the General Staff Department. The 3rd Department is primarily responsible for signals intelligence, advanced high-performing computing, and encryption. Furthermore, the department is composed of twelve operational bureaus that all serve different functions as Lindsay, Cheung, and Revoren state. The First Bureau’s mission is encryption, decryption, and other information security roles. The Second Bureau is responsible for CE against the United States because its role focuses on the United States and Canada for political, economic, and military intelligence. The Third Bureau’s job is functional intelligence, as it collects radio communications and protects border networks and emissions control. The Fourth Bureau focuses on Japan and Korea, while the Fifth Bureau focuses on Russia. The Sixth Bureau monitors Taiwan and much of South Asia. The Eighth Bureau focuses on Europe, the Middle East, Africa, and Latin America. The Ninth Bureau is responsible for high-end computing, intelligence analysis, database management, and audiovisual equipment. The Tenth Bureau focuses on Central-Asia and Russia, with an emphasis on missile tracking. The Eleventh Bureau also has a Russia related mission. The Twelfth has a functional mission related to satellites and the collection of space-based intelligence. The 3rd Department and Second Bureau are likely the primary actors responsible for economic espionage and the entire cybersecurity apparatus as

\[28\] Cheung, Lindsay, and Reveron, 170-172.
displayed in Figure 1. The whole cyber system must work together to develop an actionable and worthwhile product to Communist Party leaders and the companies seeking to benefit from the stolen information alike.

**Figure 1: China's Cyber Apparatus**

The organizational structure of the Chinese cyber system provides the basis for the below discussions on the three doctrines the 3rd Department pursues: informatization, the information

---

29 Ibid, 9.
warfare doctrine, and active offense and defense. Informatization is viewed as “a means to ensure sustained economic growth, enable China to compete globally in the information technology realm, and to ensure national security against domestic and international threats.”

Informatization is the primary and broadest goal that China pursues in general. Because a large percentage of the Chinese population lives in rural settings, technological development has lagged behind that of other industrialized countries like Russia and the United States. From China’s perspective, this has led to a national security concern because of their perceived technological inferiority, making digitization through the development of information a cost-efficient way to allow China to develop and compete in the global technology market while maintaining security against foreign and domestic threats.

Second, China’s information warfare doctrine maintains a focused guiding principle relating to cyber activities. According to Chinese writings, supremacy in information warfare can be defined as “achieving information control within a specific time and place,” and it “is the precondition for achieving supremacy in the air, at sea, and on the ground and it is critical to achieving and maintaining battlefield supremacy.” As is evidenced by these strategies, information warfare and control over cyberspace is now the leading priority for China; it is the foundational concept that all other victories and achievements are built off of. Therefore, because Chinese leadership believes information is critical to success, they would be willing to steal secrets from more technologically advanced countries in order to catch up in the digital realm. Information superiority is a global endeavor for China because it entails battlefield preparation and dominance. China must account for a panoply of international threats and contingencies so information superiority cannot be relegated to a national scope alone.

---

30 Ibid, 164.
31 Ibid, 141.
Finally, active offense and defense is a tactical doctrine used by the Chinese to achieve information supremacy. Active defense can best be thought of “as a politically defensive, but operationally offensive strategy in which China will rhetorically maintain a defensive posture up until the time it decides to attack,”32 while active offense is “based on the assertion that, unlike traditional defensive operations that can reduce an enemy’s combat power, defensive information operations merely fend off attacks without weakening the opposing side’s forces. Consequently, offensive information operations are the only way information superiority can be achieved.”33 The implications for Chinese economic espionage are clear in the active offense and defense doctrines. In keeping with the idea of active defense, China can conduct espionage against industrial targets inside the United States and other countries but rhetorically claim that no such action is occurring. This would allow them to deny any adverse consequences that occur as a result of their actions but remain prepared to continue to conduct them in the future. However, if Chinese hackers are identified, as in the case of the five indicted military hackers exposed in 2014, it weakens their claims of ignorance in future situations and the effectiveness of active defense as a doctrine decreases. Active offense is employed hand in hand with active defense. With traditional combat operations, defensive fighting is able to reduce the other side’s ability to launch further attacks in the future. However, in cyberspace, defensive operations do not reduce the other side’s ability to launch more attacks in the future. Because defense only guards one’s own networks and does not inflict damage on the other side, it must be paired with offensive actions to reduce the other side’s ability to launch attacks in the future.

Lindsay et al.’s work applies to Keohane and Nye’s theory of complex interdependence because it shows the importance that China has placed on the value of commercial and strategic

32 Ibid.
33 Ibid, 142.
information and the vast amount of resources it has dedicated as a state to obtaining such information, often through espionage. Moreover, the interconnected relationship between the General Staff Department and State Council highlights the ample opportunities that exist for communication to occur through multiple channels. While a clear delineation of Chinese state priorities is difficult to determine, the breadth and depth of CE shows that it is used as a tactic rather than a strategy. China pursues CE much like a vacuum picks up waste; they collect vast quantities of information and then make decisions based on the information later. The United States National Security Agency goes about collecting information in much the same way. Through its metadata collection program, the National Security Agency exploits acquired information to conduct target development and to identify co-travelers. Target development is a practice to find unknown associations of individuals already targeted by the National Security Agency and the co-traveler program seeks to identify people who are traveling with or planning to meet with previously identified suspects.\(^{34}\)

In addition to Lindsay et al. and Keohane and Nye, Aaron Brantly discusses the intricacies of interdependence and cyberspace. Brantly states, “Security issues within an interdependent environment increasing in absolute value with increases in connections cannot and should not be conceptualized within a purely relative gains framework.” Moreover, “National security depends on cyberspace not only for its C2W [Command and Control Warfare] capabilities but also for a multitude of systemic interconnections including economic security, environmental security, social and political security, as well as military security.”\(^{35}\)

---

\(^{34}\) “How the NSA is tracking people right now.” *Washington Post.* [https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-tracking-people-right-now/634/](https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-tracking-people-right-now/634/).

\(^{35}\) Brantly, 11-12.
As can be readily seen, Brantly’s discussion of interdependence directly ties in to the formulations Keohane and Nye create. China’s quest for sustained economic growth has led it to conduct CE in hopes of saving costs on research and development at the expense of the United States and many other developed countries. This directly relates to relative versus absolute gains. Neoliberals typically emphasize absolute gains and they focus on the absolute utility of actions and emphasize the prospect for cooperation. Realists typically employ relative gains and they focus on relative capabilities compared to other actors and they emphasize the potential for conflict.\(^{36}\) Through this particular practice, China can be seen attempting to achieve relative gains compared to the United States. However, this incidence does not necessarily eliminate all potential absolute gains, as the United States can continue to bolster its own capabilities.

Maximizing relative gains jeopardizes the security of targeted nations because economic stability and the integrity of one’s economic system are components of a nation’s national security. Former Acting Director of the Central Intelligence Agency Michael Morell states, “that the health of a nation’s economy is the single most important determinant in its ability to protect itself, the single most important determinant in its ability to project power, the single most important determinant in its national security.”\(^{37}\) Sheila Ronis adds to this dimension when she says that without capital, there is no business, without business, there is no profit, without profit,

there are no jobs, without jobs, there are no taxes, and with no taxes, there is no military capability.\textsuperscript{38}

Thomas Rid in \textit{Cyber War Will Not Take Place} establishes a basic understanding of how espionage is conducted in cyberspace and what this means for state actors. First, Rid asserts that CE “is an attempt to penetrate an adversarial computer network or system for the purpose of extracting sensitive or protected information.”\textsuperscript{39} This definition’s significance lies in the fact that it does not necessarily amount to a direct operationally offensive attack against an adversary with the intention of causing network damage; instead, its role is simply to go unnoticed to acquire the desired information.

Second, Rid explains three paradoxes relating to CE.\textsuperscript{40} The first is the danger paradox, which states that espionage is not an act of war yet it poses serious threats to the world’s most advanced economies. The second paradox is the significance paradox which holds that while CE may be the most significant form of cyber attack, it may not be that different from what the best intelligence agencies already know how to deal with. This confusing statement is explained by the third normalization paradox, which says that intelligence agencies with cyber operations will back up such actions with human sources, thus moving the operations out of the cyber realm where they started back into the physical world.

Third, Rid makes an astute point also highlighted by Lindsay et al. when discussing China’s strategy of indigenous innovation when he contends that even if China is able to steal information from the United States, it might not be able to take advantage of it because “process-

\begin{itemize}
\item \textsuperscript{39} Rid, Thomas. \textit{Cyber War Will Not Take Place}. New York: Oxford University Press, 2013, 81.
\item \textsuperscript{40} Ibid, 82-83.
\end{itemize}
related knowledge may reside more in routines and practices, not in reports or on hard-drives, and therefore seems to be more difficult to steal and to replicate remotely.\(^\text{41}\) In other words, while China might be able to steal information from countries like the United States, it might not be able to capitalize on it within its own economy because it still might be too advanced for existing infrastructure or it could lack the relevant context to be leveraged effectively.

Fourth, Rid describes three trends that have emerged with the rise of the Internet and then discusses the problems these developments pose to intelligence agencies.\(^\text{42}\) First, there is an unprecedented level of data that has never been known before. Second, attribution has become increasingly difficult to achieve. At this point, Rid and Brantly can be connected, as Brantly argues that “it is more important to identify that an attack is occurring, what the target of that attack is, and how to prevent the achievement of an attacker’s goal, than to in the moment identify who is actually conducting the attack.”\(^\text{43}\) Such diagnoses can be conducted following the conclusion of attacks, but trying to do so in the moment constricts actors to a purely defensive posture and does not provide any sort of deterrent measure to prevent attacks from occurring in the first place. Third and finally, economic and political espionage are blurred and pose distinct problems to many western democracies. In the United States, economic espionage is not a state enterprise because there would be no way to decide which companies benefit from the stolen information due to the market orientation of our economy, whereas in China, a substantial

\(^{41}\) Ibid, 85.
\(^{42}\) Ibid, 107-112.
\(^{43}\) Brantly, 87.
percentage of all companies are state owned so distributing information is a much easier task to handle.  

With the emergence of these trends, five issues have become clear at the same time: selection of the most relevant information, interpretation and analysis, reorienting and connecting human intelligence, openness to succeed, and the ability to draw the line between foreign and domestic intelligence. The ability and willingness to overcome these obstacles pose a difficult challenge to countries like the United States that are dedicated to sustaining the openness of democratic institutions and maintaining the divide between foreign and domestic operations. Efforts to solve them may result in the creation of interdependent relationships among countries that would not have existed prior to the information age.

Furthermore, economic espionage poses interesting questions for the relationship between China and the United States as their behemoth economies continue to become increasingly intertwined. If Keohane and Nye’s formulation of complex interdependence and the lack of military conflict between powers can be extended into the cyber realm, then a wholly new conceptualization of cyber complex interdependence can be achieved.

Gordon Corera provides useful context for China’s political climate in *Cyberspies*. When discussing one of the most advanced cyber operations carried out by China, Titan Rain, Corera states that the “modern Chinese Communist Party has three strategic goals: maintain social stability, defend the country and its interests and become a regional and ultimately global power. Maintaining a frenetic pace of economic growth is an imperative for all three.”

---

formulation of domestic goals outlined by the ruling party is helpful because it shows the impetus behind China’s actions. Because China seeks stability, security, and global influence, it engages in CE and targets the countries that will be most beneficial for that purpose.

Keohane and Nye, Lindsay et al., Brantly, Rid, and Corera all provide valuable insight into the field of interdependence relating to cyberspace today. I have sought to connect the literatures and engage them with one another to demonstrate that while discussion of interdependence and cyber activities occur on their own, a specific work on how Keohane and Nye’s complex interdependence model specifically relates to cyberspace is lacking. The main expectations of this work for United States-Chinese relations are to show that because multiple channels of communication exist, there is an absence of a hierarchy of issues, there is a lack of conventional military conflict, China sets its own agenda, international organizations play a role, and the United States was able to successfully demonstrate the willingness to alter the shadow of the future between the two countries, an interdependent relationship exists in accordance to Keohane and Nye’s theory of complex interdependence. I will subsequently apply Keohane and Nye’s model to interactions in cyberspace to fill this theoretical gap.

**Complex Interdependence Analysis**

Keohane and Nye’s model of interdependence revolves around the creation of multiple channels of communication between nations across economic, political, social, and military spectrums that increase the cost of initiating military action. The development of cyberspace has led to a substantial increase in the number of connections between the United States and China, particularly in the economic realm, and as such, complex interdependence theory is a useful tool in examining Chinese-American relations. Figure 2 shows that United States’ imports of Chinese goods have increased four-fold since 2000. Moreover, interdependence theory suggests that
those who conduct attacks will have serious costs imposed on them in addition to the costs borne by their victims. These costs are the result of interdependencies resulting in what Joseph Nye calls entanglement, a form of “self-deterrence.”

Keohane and Nye argue that multiple channels of communication between societies can be grouped into three categories: interstate, transgovernmental, and transnational relations. For the authors, interstate relations “are the normal channels assumed by realists,” transgovernmental relations are those that exist “when we relax the realist assumption that states act coherently as units,” and transnational “applies when we relax the assumption that states are the only units.”

---

48 Keohane and Nye, 20.
All three methods of communication are found to be present in relations between China and the United States.

First, interstate relations embody those such as formal exchanges between heads of state as well as those interactions, formal or informal, between governmental elites and offices of government such as diplomatic entities or military organizations. Henry Kissinger details how such interactions regularly occur between China and the United States when he writes, “Top American and Chinese officials have exchanged visits and institutionalized their exchanges on major strategic and economic issues. Military-to-military contacts have been restarted, opening an important channel of communication.”49 Visits to the United States by Chinese Presidents Hu Jintao and Xi Jinping demonstrate that channels of dialogue at the highest levels of government exist and that significant strategic conversation occurs where major decisions with global implications are decided. Moreover, China and the United States seem to have found avenues where cooperative relations can exist, as drills and exercises for occurrences like natural disasters allow for opportunities where both countries’ militaries can train together.50 While both nations’ defense organizations are competitors, their communication along with that of other formal foreign office actors ensures that interstate relations remain consistent.

Second, transgovernmental relations mainly constitute informal ties among governmental or nongovernmental elites, like competing government departments, prominent businesspeople, or other influential citizens. This informal dialogue is seen as more of a backdoor business where pressing issues can be resolved outside of the public eye and information can be exchanged

between societies.\textsuperscript{51} This increasingly influential form of communication can perhaps best be demonstrated through the increasingly large number of exchange students and travelers that China and the United States send abroad to each other’s country every year. As Chinese-American economic ties continue to deepen, there are about “9,000 people travelling across the Pacific Ocean every day, about 200 flights every week and more than 3 million people every year.”\textsuperscript{52} Moreover, there “are as many as 100,000 Chinese and American students studying in the United States and China every year.”\textsuperscript{53} When taking into account that approximately 13 percent of Chinese and American citizens are of college age and that a lower percentage still of this demographic attend universities, this exchange number takes on an added level of significance.\textsuperscript{54} Travel numbers between the two countries are significant because they demonstrate the level of interaction between the two societies through which ideas can be exchanged and they represent opportunities for conflict resolution conversations as well. Moreover, student exchanges are even more telling of how transgovernmental communication occurs as high-achieving students that study abroad to learn cultural intricacies and internationally-applicable skills are often bound to be the governmental, economic, and societal leaders of their generation so early exposure with the other country forms connections that can be leveraged in the future.

\textsuperscript{51} “Tracks of Diplomacy.” United States Institute of Peace. \url{https://www.usip.org/glossary/tracks-diplomacy}.
\textsuperscript{53} Ibid.
Finally, transnational relations are those that occur through organizations that operate globally. This mode of communication between China and the United States is perhaps the most obvious as America’s economy continues to globalize and outsource its manufacturing and support functions to China and other countries in the region. In *The World Is Flat*, Thomas Friedman traces the production process of his laptop computer and goes into painstaking detail to portray just how complex the global supply chain system is.\(^{55}\) In Friedman’s opinion, this interaction between organizations across nations makes interstate conflict far less likely. While this would certainly be a feather in complex interdependence theory’s cap, Richard Clarke posits the opposite.\(^{56}\) In his opinion, the supply chain for products “may in fact make cyber warfare more likely, or at least make it more likely that the Chinese would win.”\(^{57}\) When dealing with electronic products specifically, which a significant portion of trade goods between China and the United States are, at any point in the supply chain, “vulnerabilities [could be] introduced, most accidentally, but probably some intentionally, that can make [the product] both a target and a weapon in a cyber war.”\(^{58}\) While globalizing organizations definitely create additional opportunities for citizens of China and the United States to increasingly interact with one another, they also create new points of vulnerability for the products that are exchanged as a result of those companies’ business.

In summary, channels of communication between formal heads of state and other cabinet level departments indicate that interstate relations between China and the United States remains a legitimate avenue for discussion to the current day. Moreover, exchanges between governmental


\(^{56}\) Clarke and Knake, 88.

\(^{57}\) Ibid.

\(^{58}\) Ibid.
elites and rising stars in universities through transgovernmental relations indicates that these interactions are likely to continue into the foreseeable future and they also provide both governments with additional tools to secure the outcomes they want. Finally, global business practices provide citizens with opportunities to interact with those at their own level in other countries in a way that never existed before the information age. While this development contains many positive forces for significant change, it also generates points of vulnerability for societies that also did not have to be accounted for before the age of globalization. As such, the first requirement of complex interdependence seems to hold between China and the United States.

Absence of Hierarchy of Issues

In addition to multiple channels of communication, complex interdependence also insists that the “agenda of interstate relationships consists of multiple issues that are not arranged in a clear or consistent hierarchy.”  

Between China and the United States, such a void of hierarchy does seem to exist as the members of the world’s most influential bilateral arrangement must juggle the stress of the absence of a common enemy, trade differentials that are detrimental to the United States, tensions in the East and South China Seas, and competing interests dealing with Taiwan and North Korea.

Following the Soviet Union’s emergence as a world superpower after World War Two and Mao Zedong’s victory in the Chinese Civil War in 1949, a tripolar security environment emerged in Asia as China, the United States, and the Soviet Union all strove to protect their own

59 Keohane and Nye, 20.
interests. However, as the Cold War heated up and tensions between the differing forms of Sino-Soviet communism became more acute, China and the United States found themselves in a position to work cooperatively in order to curb Soviet influence. While Soviet expansion was threatening to both the United States and China, there were events during the Cold War that caused tensions between China and the United States as well. For example, the Korean and Vietnam Wars both entailed large-scale conflicts being fought on immediate Chinese borders. President Richard Nixon and Secretary of State Henry Kissinger also dedicated significant efforts to opening China, actions which were intended to bring peaceful relations between Washington D.C. and Beijing, stability to East Asia, a relaxation of Cold War tensions with the Soviet Union, and an end to the Vietnam War.\(^\text{61}\)

While such an arrangement ended up being beneficial to both parties during the 20\(^{th}\) century, such an environment no longer exists today as there is no significantly formidable adversary for both sides to ally against. Instead, China and the United States can both focus on the actions and intentions of each other without a significantly powerful adversary on par with the Soviet Union being in the immediate picture.

Second, a common theme throughout President Donald Trump’s 2016 campaign was that the existing trade equation between China and the United States was grossly skewed in favor of China’s interests. The United States has incurred a more than $300 billion trade deficit with China. Such a differential requires long-term planning and patience to correct, which does not lend itself to success in the current world environment where conditions are constantly shifting and where more pressing complications requiring short-term decisive action present themselves on a daily basis. The existing trade deficit can also be analyzed in the context of relative versus absolute gains. In this instance, China is able to collect relative gains compared to the United

---

States because it is able to increase its sales potential and increase its profits. However, there is also potential for absolute gains to be made in this relationship. By importing a large amount of products, the United States is able to introduce new products to the market, reduce costs, become a leader in certain industries, and provide quality products to its customers.

Third, the East and South China Seas have become increasingly militarized and present themselves as a potentially serious flashpoint for conflict between China, Japan, Vietnam, the Philippines, Indonesia, Malaysia, and Taiwan. Japan has claimed control over islands in the East China Sea since the 1970s but their legitimate possession is being challenged by China as the People’s Republic seeks to expand its global power projection capability. Moreover, the South China Sea contains some of the world’s most important shipping lanes as more than $5 trillion of seaborne trade passes through this region. Furthermore, two of China’s closest competitors, Taiwan and Japan, rely extensively on imports for resources so if China choked them out of the region, it could exert an enormous amount of influence over their operations from that point forward.

Fourth, Taiwan presents Beijing and Washington with a very controversial and stressful situation. China has forthrightly claimed that if Taiwan seeks independence, it will not hesitate to invade the island to ensure that it remains part of China. On the other hand, America has long supported Taiwan as a sovereign entity through arms sales and other forms of recognition.

Fifth and finally, North Korea presents China and the United States with both a challenge and an opportunity to work together. On one hand, China definitely wants to maintain its control

---

63 Ibid.
over North Korea just as the United States aims to maintain its suzerain status over Israel. On the other hand, both great powers recognize that North Korea as an isolated and nuclear-equipped state is not in the long-term best interest of either nation. A critical balance between maintaining respective strategic interests and preventing oneself from becoming unilaterally responsible for the restoration of North Korea to the world stage seems to be in the process of being struck.

The loss of a common enemy, trade imbalances, the East and South China Seas, Taiwan, and North Korea all constitute foreign policy issues to be addressed by China and the United States. However, there are also domestic goals that each country deals with on small and large scales. For example, economic growth is an almost globally sought after goal and China and the United States both seek to continue to further their economies. However, because other pressing issues are closely interconnected with the economy, it does not mean that economic concerns supersede those other concerns. This intertwined relationship itself between economics and national security, for example, shows that a clear and distinct hierarchy is difficult to wholly recognize. The collective groups of issues are addressed in turn and each certainly merits focused individual attention by policymakers.

To reiterate, the loss of a common enemy, trade imbalances, the East and South China Seas, Taiwan, and North Korea all present the United States and China with issues on the agenda to be solved. How the two powers go about settling the differences on these issues will likely transform the balance of power in the Asia-Pacific region. While such a conclusion is decidedly realist in nature, the lack of a hierarchy among all of these issues also satisfies the second requirement of complex interdependence theory and demonstrates that the two schools of thought are not mutually exclusive in this instance.

---

Minor Role of Military Force

The third criterion for complex interdependence, in addition to multiple channels of communication and the absence of a hierarchy of issues on the agenda, is the relatively minor role of military force used between two states. With this point of emphasis, interdependence theory takes its clearest departure from the predominant realist thinking of its day, as securing power is no longer the overriding concern of states in Keohane and Nye’s minds, although it remains a central component of national power. On this point, Keohane and Nye note that “particularly among industrialized, pluralist countries, the perceived margin of safety has widened: fears of attack in general have declined, and fears of attacks by one another [original emphasis] are virtually nonexistent.”66

Approaching this point from the view of China and the United States, it is true that there has not yet been a broad rise of conflict between the two powers since the Korean War. However, this relative conventional peace should not overshadow the rapid buildup of Chinese military capacity across the mainland, South China Sea, ports across the Indian Ocean, and military logistics locations across the continent of Africa. The United States also engages in military modernization practices, but modernization is a normal, core part of military action along with force structure, readiness, and sustainability.67 The role of military force can also be analyzed in a relative versus absolute gains framework. The absolute gains available to both sides show that advancement is possible for both the United States and China. However, the relative gains indicate that China is developing specific technologies to give it an edge against adversaries like the United States. This development is occurring through what is called

66 Keohane and Nye, 23.
intelligence-ization, which is the incorporation of intelligent technologies into weapons and equipment. Some of these new technologies include artificial intelligence, big data, quantum communications and computing, nanotechnology, hypersonic vehicles, directed energy weapons, battlefield robotics, and technologies based on new physical principles that can drastically change warfare. Military expenditures are based on relative gains as countries, like both China and the United States, seek to develop advantages in their own capabilities to counter the technology of competitors, but there are also absolute gains available for both sides like advancements in force structure, modernization, readiness, and sustainability. Even more so, while conventional kinetic force has not been used between China and the United States, CE has been used extensively which has blurred the line between traditional intelligence gathering techniques and cyber war.

In *Cyber War*, Richard Clarke defines cyberwar as “the unauthorized penetration by, on behalf of, or in support of, a government into another nation’s computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls.” The United States and China have allowed the role of force in cyberspace to play a major role as China has targeted and successfully penetrated one of America’s most vital and vulnerable sectors, the electric power grid. In the event of a military conflict between the two nations, China could potentially compromise America’s critical infrastructure. A report by the cybersecurity firm Mandiant “found that hackers working on behalf of the Chinese government

---


69 Ibid.

70 Clarke and Knake, 228.
were able to penetrate American public utility systems that service everything from power
generation, to the movement of water and fuel across the country.”\textsuperscript{71} To delve into further detail,
head of United States Cyber Command and the National Security Agency Admiral Michael
Rogers is quoted as saying ““We see them attempting to steal information on how our systems
are configured, the very schematics of most of our control systems, down to engineering level of
detail so they can look at where are the vulnerabilities, how are they constructed, how could I get
in and defeat them.”\textsuperscript{72} If China were to shut down the three American power grids, the action in
itself would not necessarily be violent or constitute a loss of life. However, the immediate effects
of such an attack and future potential ramifications could prove to be catastrophic for American
society as the banking, food, transportation, and utility sectors and many other critical services
rely on electricity to function. The insertion of Chinese malware into American critical
infrastructure can be definitively viewed as a statement of hostile intent from the American
perspective. From the viewpoint of the party whose network has been penetrated, it is impossible
to determine whether a foreign actor has intruded into your system for offensive or defensive
purposes.\textsuperscript{73} This inability to identify an actor’s motives can lead to dangerous situations where
the targeted country responds in a disproportionate or inadequate manner.\textsuperscript{74} Based on the
prevalence of such actions, it would not seem that the third stipulation of complex
interdependence theory holds between China and the United States. However, the absence of
conventional conflict between the two powers and the decline in CE since 2014 seem to indicate

\begin{footnotes}
\textsuperscript{71} Crawford, Jaime. “The U.S. government thinks China could take down the power grid.”
\textsuperscript{72} Ibid.
\textsuperscript{73} Buchanan, Ben. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.
\textsuperscript{74} Brantly, Aaron. “Aesop’s Wolves: The Deceptive Appearance of Espionage and Attacks in
\end{footnotes}
that military force does not play a major role between China and the United States so the third
stipulation of complex interdependence theory holds.

Linkage Strategies

Having discussed the three core principles of complex interdependence and analyzed
them in the context of the Chinese-American relationship, a similar process will be used to
investigate whether the political processes associated with complex interdependence are also
applicable. First, Keohane and Nye discuss linkage strategies and argue that “as the utility of
force declines, and as issues become more equal in importance, the distribution of power within
each issue will become more important. If linkages become less effective on the whole,
outcomes of political bargaining will increasingly vary by issue area.” In practice, an example
of China attempting to link two issues together is occurring where as its domestic economy has
begun to slow down, it has attempted to increase force projection abroad.

Because of China’s communist system of government, a substantially high percentage of
the country’s companies are state owned enterprises whose output has begun to decline in recent
years. Primarily, this is a result of the fact that almost all of these state owned organizations are
industrially oriented and China’s economy has started to transition to a service-based system as a
whole. China has sought to replace the declining rate of domestic market growth with
international military and economic projects that can be used to replace the pride once found in
the high growth rates of its economy. When Deng Xiaoping led China, his spending position
held that economic development efforts should take priority over military spending. However,

75 Keohane and Nye, 26.
76 Tan, Huileng. “China’s economic problems are exactly why its global influence is
Chinese security spending now outpaces the rate of national economic growth.\textsuperscript{77} The Chinese legislature approved an increase in the People’s Liberation Army budget of 8.1 percent for next year.\textsuperscript{78} Moreover, spending on domestic security services increased by 17.6 percent and 12.4 percent respectively in 2016 and 2017.\textsuperscript{79} This compares to an economic growth rate of about 6.5 percent or less, which means total security spending is at least double the pace of economic growth and could be triple the amount based on the accuracy of available figures.\textsuperscript{80} This is important because it shows that major investments are being made into the Chinese security apparatus while economic growth rates are stagnating and lagging behind.

A major effort has been made to promote the new and expanding One Belt, One Road project. This behemoth investment program’s aim is to create a continuous high-tech and digital silk road across Asia and Africa in order to present Chinese companies with new consumers in order to sustain declining growth.\textsuperscript{81} Moreover, locations for the project are selected based on strategic dual use interests where the Chinese government can claim that ports and bases are solely for economic transactions, but they can easily be seen to quickly transform into forward military operating bases when desired. For example, in Sri Lanka, Greece, and Djibouti, “Chinese investment in civilian ports has been followed by deployments or visits of People’s Liberation Army Navy vessels and in some cases announcements of longer term military


\textsuperscript{78} Ibid.

\textsuperscript{79} Ibid.

\textsuperscript{80} Ibid.

contingencies.” Furthermore, “There is an inherent duality in the facilities that China is establishing in foreign ports, which are ostensibly commercial but quickly upgradeable to carry out essential military missions.” This makes these ports useful for various Chinese missions when the need arises.

In sum, China relied on its expanding economy and global investment for much of its rise to power in the 1990s and early 2000s. However, as growth rates have proven unsustainable over the long run, a renewed and concerted effort is being made to reinvest in China’s global military and economic capacity. China’s economic growth rates do outpace those of the United States, but diminishing growth rates on a smaller economy are smaller in the long run than a consistent growth rate in a larger economy. While the expansion of Chinese military expenditures and capabilities might not be a direct result of declining economic growth, the two phenomenon definitely correlate and likely support one another. Chinese leadership has worked to substitute the newfound military capability for the pride once placed in the economy, and that being the case, a successful linkage strategy seems to have occurred where an economically great state was able to leverage its position to rise to power militarily and economically abroad, thus providing evidence against Keohane and Nye’s linkage strategy process.

*Agenda Setting*

Following the formation of linkage strategies, Keohane and Nye posit that under complex interdependence, “we can expect the agendas to be affected by the international and domestic problems created by economic growth and increasing sensitivity interdependence.” In order to understand this situation, a more detailed discussion of sensitivity interdependence is warranted.

---

83 Abhijit Singh, as cited in Bokhari, et al.
84 Keohane and Nye, 27.
Keohane and Nye state that sensitivity interdependence can provide “the basis for significant political influence only when the rules and norms in effect can be taken for granted, or when it would be prohibitively costly for dissatisfied states to change their policies quickly. If one set of rules puts an actor in a disadvantageous position, that actor will probably try to change those rules if it can do so at a reasonable cost. Thus, influence deriving from favorable asymmetries in sensitivity is very limited when the underlying asymmetries in vulnerability are unfavorable.”85 Currently China can be seen acting in the international system by expanding into and claiming islands of the East and South China Seas as well as building rail systems across the continent of Africa. Such behavior has thus far occurred largely unchallenged and allowed China to become predominant in the African mineral trade. However, these two events are not in the exact same category of challenges to the international system although they both show engagement on the global stage. Involvement in the East and South China Seas involves expanding territorial claims and contests with neighboring countries, while the rail systems and mineral extraction denote foreign direct investment for political utility and economic development.

Returning to Keohane and Nye’s first point on agenda setting in that it is related to issues associated with economic growth, China’s expansion into the African mineral market is a prime example of such behavior. Over the last two decades, China’s rapidly expanding and industrializing economy has consumed vast quantities of natural resources that are now very scarce in its homeland. The transition from an industrial economy into a service economy is forcing China to search for resources abroad and Africa has proven to be fruitful.

China’s strategy across the continent has been labeled “Two Resources, Two Markets” as it seeks to connect its own depleting domestic mineral reserves with Africa’s blooming markets

85 Ibid, 15.
and reserves. The project broke ground in 2006 and in less than ten years, “the number of major mining/mineral processing assets in Africa with China-headquartered companies interest, increased from only a handful in 2006 to more than one hundred and twenty in 2015.” Figure 3 displays the expansion of Chinese investment in the African mineral trade since 2006 and two categories of resources are worth mentioning specifically. First, uranium mining conducted by China is significant because it provides reserves for expanded civilian nuclear programs in China’s future. Second, base and precious metals make up the largest category of materials sought after. These materials are the building blocks of almost all electronic equipment today so having large amounts of these metals provides China with a strategic economic productive edge compared to its competitors.

Part of what makes China effective in capitalizing on the African mineral trade is their use of another side of cyber theft that is not as apparent: stealing business sensitive information. “It might relate to contracts, mergers, and acquisitions or bids.” Furthermore, “mining is one industry that is believed to have been hit hard over contract negotiations. Companies trying to buy up a copper mine in the Congo might find themselves losing out but not realising [sic] they had been outbid by a fraction based on inside knowledge.”

---

88 Ibid.
89 Corera, 195.
90 Ibid.
In sum, China’s economic boom over the last two decades caused it to exhaust many of its domestic reserves of useful materials for the sake of its industrial expansion.\textsuperscript{91} The reserves-to-production ratio estimates the burn rate of proven reserves of mineral commodities and China is in the “red zone” for nearly all mineral commodities found at home.\textsuperscript{92} This has forced a global expansion for when the reserves are completely exhausted or it becomes too expensive to continue to use the national reserves. China is now shifting its political agenda to account for growing needs for resources. To accomplish this goal, China expanded into the East and South China Seas in order to access gas and oil fields and it created the Two Resources, Two Markets program in Africa to secure strategic precious resources.\textsuperscript{93} All of the above actions present evidence that Chinese politics of agenda formation have taken on added importance with all of the issues that face the country’s leadership today, so the second political requirement for Keohane and Nye appears to be confirmed.

\textsuperscript{91} Basov, Vladimir. “China is burning through its natural resources.” Mining. April 26, 2015. \url{http://www.mining.com/china-burning-natural-resources/}.
\textsuperscript{92} Ibid.
Transnational and Transgovernmental Relations

The third political consideration for complex interdependence theory deals with the role played by transnational and transgovernmental relations. Reverting back to the three foundational tenets of the theory, transnational and transgovernmental organizations play a role in creating and securing multiple channels of communication through society which undercuts the traditional realist conception that communication can only occur at the premier echelons of government. Keohane and Nye contend that the existence of multiple channels “leads us to expect limits, beyond those normally found in domestic politics, on the ability of statesmen to calculate the manipulation of interdependence or follow a consistent strategy of linkage. Statesmen must consider differential as well as aggregate effects of interdependence strategies and their likely implications for politicization and agenda control.” While it may at first glance seem that because multiple channels exist between China and the United States that this condition must be fulfilled also, further investigation is required. Namely, while China allows for

---

94 Basov, The Chinese scramble.
95 Keohane and Nye, 28.
governmental and economic elites to communicate with their United States counterparts for business purposes, the same cannot be said for domestic Chinese actors’ ability to manipulate the government’s agenda. Some companies, like technology giants Alibaba and Huawei, collect tremendous profits but in the process attract close government scrutiny. Many of China’s top companies are state owned, and as soon as a company becomes significant, the government likes to become involved in its ownership or operations.96

While the government does seek to monitor and control situations that could potentially undermine its power, certain organizations are able to manipulate the relationship and establish a bidirectional connection. This is done through asking the government to protect Chinese citizens abroad, asking the government to influence economic policies abroad to protect Chinese investments and to make sure Chinese loans are repaid, asking to have the government leverage cross-border deals against debtors to advance other interests, and asking for the government to act on other international issues that could expand its influence in the economic realm.97

China’s unique ability to control which issues are politicized and the priority of its agenda lie in the system of government employed and the ability to constantly be monitoring its citizens through cyberspace. Luo finds that public agendas through online forums are not able to affect the policy agenda at the national level, although they do have some influence when dealing with specific isolated incidents. Instead, the national policy agenda plays a very significant role

in shaping the public agenda and discussion on public online policy forums. First, China is attempting to install Green Dam software “on all of its computers, allegedly to screen for child pornography and other prohibited material.” It “could also scan for malware installed by enemy states.” Moreover, in addition to the Green Dam, China employs the Great Firewall of China, which is a program that “screens traffic on ISPs [Internet Service Providers] for subversive material… The system engages in something called ‘Domain Name System hijacking,’ sending you to a Chinese government clone of a real site when you are in China.” What makes the Great Firewall so effective “is not only its complex technology but also the culture that the system engenders – a culture of self-censorship.” Furthermore, it has the ability to disconnect the Chinese Internet from the global Internet. Taken together, the Green Dam and Great Firewall of China play a dramatic role in curbing the influence of transnational and transgovernmental organizations in setting the Chinese political agenda. Instead, because the Chinese Communist Party maintains a secure grip on civil society groups and because such a large percentage of companies are state owned enterprises, Chinese leadership directs organizations in which direction to go and they are then subservient to the State’s wishes. In light of these findings, the third political requirement for complex interdependence theory does not seem to be met.

---

99 Clarke and Knake, 56.
100 Ibid.
101 Clarke and Knake, 56-57.
Role of International Organizations

Lastly, the final political consideration for Keohane and Nye regarding complex interdependence is the role played by international organizations. For the authors, “in a world of multiple issues imperfectly linked, in which coalitions are formed transnationally and transgovernmentally, the potential role of international institutions in political bargaining is greatly increased. In particular, they help set the international agenda, and act as catalysts for coalition-formation and as arenas for political initiatives and linkage by weak states.”  

In the United States, two broad movements help set the international agenda when it comes to policy regarding China: environmental activists and human rights advocates.

China’s rapid economic rise has come at the expense of the environment because of industrialization. Concretely, China is the world’s largest source of carbon emissions and many of its cities fail to meet international health standards. The leading cause of China’s dire environmental situation is its status as the world’s largest coal producer and it accounts for more than half of global consumption every year. As of 2016, China has 194 million cars on the road, which further exacerbate its pollution problems, in addition to contributing to urbanization.

---

104 Keohane and Nye, 29.
Lastly, China contains nearly 20% of the world’s population but only 7% of its fresh water reserves so water depletion and pollution are two more major sources of degradation.¹⁰⁹

In response to these widespread and pressing issues, organizations like the United States-based Environmental Defense Fund work to combat this problem. This nonprofit organization has consulted the Chinese government for 25 years and has recently worked to help operate a national carbon trading program, expand the use of renewable energy, strengthen environmental enforcement regulations, improve energy efficiency in major sectors, and enhance energy modeling to impact policy.¹¹⁰ Having a United States-based nonprofit organization act as the impetus behind the formation of an environmentalist coalition describes the role outlined by Keohane and Nye, and shows that such organizations do have an impact.

In addition to environmentalist groups, human rights organizations also have an outspoken and weighty voice when it comes to Chinese affairs. When compared to Western standards of human rights, China has a poor track record of guaranteeing its citizens the same privileges that many throughout the world enjoy.¹¹¹ More specifically, China tightly restricts the freedom of expression, the freedom of religion, and women’s rights.¹¹²

As mentioned previously when discussing the role of transgovernmental and transnational organizations in agenda setting, China actively works to reduce its citizens’ ability to access information from around the world. By installing Green Dam software on all devices

and sustaining the Great Wall of China, the Chinese government attempts to control most access to subversive online discourse.\textsuperscript{113} While Chinese citizens are fairly free to criticize their government online, any efforts made to mobilize movements to demonstrate dissatisfaction with the ruling party are quickly quashed with overwhelming force.\textsuperscript{114}

Second, China severely limits the freedom of religion within its borders and in regard to Tibet as well. The Chinese Communist Party only allows access to five state-ordained religions and all meetings must be conducted in sanctioned meeting spaces. All other actions are strictly prohibited and considered contrary to the interests of the State. Moreover, China has long repressed the Uyghur Muslims in Xinjiang and considered them domestic terrorists and has taken actions in fulfillment of such labels.\textsuperscript{115} Lastly, Tibetan nationals are constantly subject to surveillance by Chinese authorities and their rights to movement and free expression of thought and religion are tightly restricted.\textsuperscript{116} Because the Chinese government considers religious thought in general as a negative force for the progression of the country, it works to limit its influence wherever possible.\textsuperscript{117}


\textsuperscript{116} “China and Tibet.” \textit{Human Rights Watch}. \url{https://www.hrw.org/asia/china-and-tibet}.

Third, China ranked 100th out of 144 nations in a World Economic Forum report on gender parity for 2017.118 This ranking has steadily been declining over the last decade as the government moves to crack down on other areas of human rights in order to solidify the power of the state. All of the above human rights violations are well documented by the international community and there are many organizations that work to reverse the continually tightening trend. One such entity is the nongovernmental organization, Human Rights in China. With offices in Hong Kong and New York, this association’s goal and mission is to “raise international awareness of and support for the diverse and expanding civil society activism in China. To accomplish these goals, [they] engage with a wide range of high-level authorities, including United Nations human rights bodies and national governments, as well as the business community and international media outlets.”119 Because China conducts and enforces such a strict domestic agenda, international organizations strive to play an important role in exposing and working to remediate abuses of otherwise internationally agreed upon standards of government-to-citizen interactions. Keohane and Nye state that through trying to define the salient issues and influence governmental priorities, organizations may be successful but will not necessarily always achieve their stated goals.120

Taken together, the examples of environmental groups and human rights advocates show that international organizations engage in political bargaining and possess influence when it comes to raising awareness about specific issues. Moreover, the ability to choose the organizational forum and time for issues is proving to be an important source of political power

120 Keohane and Nye, 29.
so the role of these groups is likely to increase in the future.\textsuperscript{121} Therefore, because coalition-forming behavior does occur, it seems that Keohane and Nye’s conception of how international organizations will behave in complex interdependence based relationships holds.

\textit{Power, Sensitivity, and Vulnerability}

Keohane and Nye argue that power “can be thought of as the ability of an actor to get others to do something they otherwise would not do (and at an acceptable cost to the actor).”\textsuperscript{122} Additionally, they discuss how states that seek to operate effectively within complex interdependence must be able to work cooperatively with prominent domestic groups and operate efficiently within the international system. Two examples of this occurring are when the United States government worked with Google following a Chinese intrusion in cyberspace and how China disregarded an unfavorable ruling regarding the United Nations Convention on the Law of the Sea.\textsuperscript{123}

Operation Aurora was a sophisticated cyber campaign carried out by the Chinese government against numerous American companies including Google, Northrup Grumman, Yahoo!, Symantec, Adobe, and Dow Chemical.\textsuperscript{124} The intrusion was revealed January 12, 2010. The attack was highly sophisticated and appears to have been undertaken with mixed motivations. In \textit{Cyber War Will Not Take Place}, Thomas Rid states, “The attacker’s motivation for the intrusion into the systems of the California search giant seemed to combine international

\begin{itemize}
\item \textsuperscript{121} Keohane and Nye, 31.
\item \textsuperscript{122} Keohane and Nye, 10.
\end{itemize}
economic espionage as well as domestic political surveillance of activists.”

Furthermore, “Aurora, unusually, was a multi-purpose attack. It exploited a previously known vulnerability in Microsoft’s Internet Explorer. Once inside an organization, the attackers used another clever technique, called man-in-the-mailbox—a pun on man-in-the-middle attacks—where an attacker would send emails that allegedly came from trusted colleagues, thus tricking others into opening attachments.”

This persistent threat constituted a major counterintelligence success for the Chinese government, as it was able to use advanced techniques to uncover the identities of agents working within the United States and cooperating with the United States government.

Once Google had discovered the breach, they worked closely with the Federal Bureau of Investigation to investigate the matter and the National Security Agency’s Information Assurance Directorate helped repair damage. This cooperation demonstrates a government-domestic group power interaction that was leveraged effectively in order to ameliorate a threat.

While Operation Aurora shows domestic power at work, China’s disregard for an international ruling concerning the United Nations Convention on the Law of the Sea shows a major actor exerting power within the international system for its own devices. In 2013, the Philippines brought a case against China in the Permanent Court of Arbitration concerning “the role of historic rights and the source of maritime entitlements in the South China Sea, the status of certain maritime features in the South China Sea, and the lawfulness of certain actions by

---

125 Rid, 148-149.
126 Rid, 149.
China in the South China Sea that the Philippines alleged to be in violation of the
Convention.\textsuperscript{129} Three years after the beginning of the case, a final ruling against China was
handed down. China had refused to participate in the case over the duration of the arbitration and
it did not accept the conclusion.\textsuperscript{130}

The primary treaty involved with this case is the United Nations Convention on the Law
of the Sea and China and the Philippines are both signatories. The Philippines brought forth the
case because China was extracting natural resources from areas that the Philippines had
exclusive economic rights to.\textsuperscript{131} China rejected The Hague’s ruling that it has no claim to these
areas and therefore showed defiance and power in opposition to an international institution.\textsuperscript{132}
While China certainly has the prerogative to not comply with the decision, its actions very well
could alienate it further from its Asian neighbors and create negative consequences for its
interdependent relationships abroad if further lawsuits are filed.\textsuperscript{133}

China continues to demonstrate its power capabilities through cyber action and it is
useful to examine where manifestations of sensitivity and vulnerability may exist. Keohane and
Nye say that sensitivity “refers to the costly effects of cross-border flows on societies and
governments, within an unchanged framework of basic policies. It is one step more than

\begin{flushleft}
\textsuperscript{129} The South China Sea Arbitration: The Republic of Philippines v. The People's Republic of
\textsuperscript{130} Ibid.
\textsuperscript{131} Bowcott, Owen, Oliver Holmes and Tom Phillips. "Beijing rejects tribunal's ruling in
\textsuperscript{132} Ibid.
\textsuperscript{133} Heydarian, Richard Javad. “Can China Really Ignore International Law?” National
\end{flushleft}
interconnectedness: interconnectedness with costly effects.”\textsuperscript{134} In the case of China and the United States, because so much of the Chinese economy depends on the stability of the United States, attacks by either side will prove to be increasingly costly for the other as their industrial and trade processes become more closely intertwined moving into the future.\textsuperscript{135} For example, in June 2017, China reclaimed its place as the United States’ biggest creditor—China possesses $1.15 trillion of the United States’ debt, $600 billion more than the closest competitor, Japan.\textsuperscript{136} Furthermore, the United States’ trade deficit with China for 2017 was $375 billion dollars, thus demonstrating how reliant on Chinese markets the United States has become.\textsuperscript{137} The statistics above demonstrate sensitivity for the relationship between China and the United States because Chinese purchases of United States Treasury Bonds impact the amount of interest the United States must pay, yet the United States continues to spend, import, export, and sell debt in the same way it always has.\textsuperscript{138} Because the basic policies between the two countries have remained largely unchanged yet produce costly effects, there is sensitivity.

Relating to sensitivity, vulnerability “is another step further in cost. It refers to the costs of adjusting to the change indexed by sensitivity, by changing one’s own policies.”\textsuperscript{139} A prime example of United States’ vulnerability lies in the relationship between China and North Korea and the latter’s development of nuclear weapons. The United States historically has been

\textsuperscript{134} Keohane and Nye, 232.
\textsuperscript{139} Keohane and Nye, 233.
sensitive to the development of North Korean nuclear weapons as it sought to maintain peaceful relations with China while pushing non-proliferation on North Korea. However, North Korean missile testing has increased rapidly since the beginning of 2017 and this has produced a costly effect in response to which the United States must react and change policies.\(^{140}\) As the North Korean missile program develops, the United States has had to repeatedly go to the United Nations Security Council asking for increased economic sanctions on the regime, and is also now considering holding talks with North Korea about the status of its nuclear program.\(^{141}\) The above demonstrates that the United States is directly vulnerable to actions by North Korea, which is heavily influenced by China. The United States is vulnerable to a nuclear-equipped North Korea because it now has to account for an additional significant external threat. This presents America with an unmitigated vulnerability without substantial help from any other world actors. The United States’ goal in this situation is to have a reversion to the status quo with the denuclearization of North Korea.\(^{142}\) Such a conclusion would reduce United States’ perceptions of vulnerability to both China and North Korea, although it would not necessarily bring an end to sensitivity between the three countries.

**Chinese Cyberespionage Analysis**

The preceding section on the nature of the Chinese-United States interdependent relationship seeks to compare the actions of China and the United States against the framework outlined by Robert Keohane and Joseph Nye in their book *Power and Interdependence*. With the


examination complete, I now turn to investigate the concrete actions of China in cyberspace as they pertain to the United States.

According to Valeriano and Maness, the “Chinese are the most active propagators in cyberspace,” and China’s favorite target is the United States.\textsuperscript{143} What this means is that in Valeriano and Maness’ tabulation of cyber incidents and disputes, China initiates the most intrusions into other countries’ networks and its most commonly targeted state is America. To conduct these cyber operations against the United States, China uses CE “because it is the least it can do without outright provocation of its more powerful competitor, the United States. China is a rising power not only in East Asia, but globally. It must be wary of its power projection with Japan, South Korea, and Taiwan regionally and with the United States globally.”\textsuperscript{144} As China developed, a cost-effective way to gain ground on more advanced countries was to engage in CE to save resources spent on research and development. The practice of espionage against adversaries for the purposes of national security is an ancient art and the United States certainly does so to gain knowledge about foreign military capabilities. However, the one big difference in Chinese cyber activities is that they engage “not just in espionage and battlefield preparation, but also in the theft of trade secrets, intellectual property, and cash.”\textsuperscript{145}

To effectively steal secrets from the United States, China bases its espionage model on a three-step process: acquisition, absorption, and application.

\textsuperscript{144} Ibid, 91.
\textsuperscript{145} Kaplan, 224.
In the acquisition step, Chinese cyber actors gain access to the information that intelligence customers seek and then recover it to China where it can be analyzed and disseminated. In the second absorption step, the stolen information is analyzed and then given to domestic Chinese institutions so they can then produce their own products without the hassle of spending time and money on research and development. During the third application step, the domestic products are transported to markets and China achieves a competitive economic advantage over its opponents. At the bottom line, China engages in economic espionage against the United States because it has found a useful avenue to do so in cyberspace and because it gives domestic Chinese organizations a competitive economic advantage.

Since the rise of cyberspace, companies and governments have been using it for their own advantage. Throughout the first decade-and-a-half of the 21st century, China conducted CE against the United States with little to no repercussions. However, according to a report produced

---

Cheung, Lindsay, and Reveron, 54.
by the cybersecurity firm FireEye, Chinese intrusions against the United States began to decline steadily in May 2014 from their previously inflated levels.

![Figure 5: Active Chinese Network Intrusions](https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf)

To discover the cause behind this sudden change in strategy, I posit five different possible causal mechanisms or events that could have precipitated this change by the Chinese cyber apparatus. It is unlikely that any one of these events in isolation caused a change in Chinese CE. Instead, a combination of factors working over time likely demonstrated U.S. resolve to end this practice and China acted in response to each of these events. First, the handing down of indictments by the United States Department of Justice against five People’s Liberation Army hackers in May 2014.

2014 could have stopped the spying. Second, the threat of sanctions issued by the Obama administration in September 2015 could have caused a change. Third, Chinese leadership perhaps thought that they no longer were behind in research and development compared to the United States so they no longer needed to engage in CE. Fourth, there could have been a shift in Chinese political and military doctrine that prioritized other methods of information collection over CE. Fifth and finally, both the Chinese and United States governments could have dutifully executed the new steps outlined at the Presidents Obama-Xi conference in September 2015.

These mechanisms relate to complex interdependence in a number of ways. First, the decision to bring light to the issue shows that the United States decided it was willing to change the shadow of the future with China and possibly affect the level of interdependence between the two countries in doing so. Second, a result of these public actions taken by the United States is that the U.S. government was acknowledging that it was sensitive and vulnerable to these Chinese practices so the reactions were a way of signaling that the United States was working to change those sensitivity and vulnerability levels. The above list of explanations for the decline in Chinese CE is not exhaustive nor are the explanations mutually exclusive. It is very likely that

150 “Is China a global leader in research and development?” *Center for Strategic & International Studies.* https://chinapower.csis.org/china-research-and-development-rnd/
several factors contributed toward China changing its CE strategy and the following discussion seeks to bring forth the impact each of the above mechanisms may have had.

*Indictments*

On May 19, 2014, the United States Department of Justice handed down indictments against five members of the People’s Liberation Army in what was the first occurrence of criminal charges being filed against state actors for hacking. The charges were issued “for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries.”\(^{152}\) Moreover, the indictments handed down by the grand jury allege that “the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises.”\(^{153}\) These actions carried out by state supported actors demonstrate the complexity and advanced nature of Chinese cyber operations. The hackers most likely maintained access to the computer networks with sensitive information by inserting a trapdoor, which is “Unauthorized software maliciously added to a program to allow unauthorized entry into a network or into the software program.”\(^{154}\) Once the hackers achieved initial access to the companies’ programs, they were then able to continue to monitor information passed on their programs because they posed as authorized users for the system.

If the indictments handed down by the Department of Justice served as a shift in Chinese CE, then one would expect to see sustained levels of spying leading up to May 2014 and then a steady decline following the announcement of charges filed, since this would bring wide public

\(^{152}\) Department of Justice, U.S. Charges Five Chinese Military Hackers.

\(^{153}\) Ibid.

\(^{154}\) Clarke and Knake, 289-290.
attention to the issue. Referencing Figure 5 above, it appears that Chinese CE began to decline significantly as the indictments became public, so they appear to have had a significant impact. This impact was a result of the U.S. signaling that CE would no longer be an overlooked practice. This in turn contributed to a deepened knowledge of the extent of violations uncovered by the U.S. for the Chinese. As a result, the indictments were the first very public admonition of CE by the U.S. so they brought along the loss of anonymity for the Chinese. A simple illustration best demonstrates the effect of the loss of anonymity for the Chinese. China and the U.S. can be imagined to be playing a game of chess in the dark. In this scenario, neither side should understand the other side’s strategy until the moves have been revealed and the lights turned back on. However, the U.S. could find a way to observe Chinese strategy during play and so understand how they are doing what they are doing. In the same way in the real world, the U.S. was able to observe China stealing American intellectual property and publicly report that China had been cheating at the game the whole time. When this came to light, China was forced to reorganize its efforts and start from scratch.

Sanctions

President Barack Obama began to consider issuing economic sanctions against organizations and individuals engaged in CE against the United States in April 2015 following the 2014 indictments of five People’s Liberation Army members. According to executive order, the financial assets of anyone engaging in malicious cyber activity against the United States can be frozen if what they are doing poses “a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.” Such a threat can clearly

be read as potentially impacting Chinese state owned enterprises since they would be acquiring American economic information for the benefit of domestic companies. Furthermore, because they are state owned companies, sanctions would directly detract from revenue for the Chinese government so they would be avoided if at all possible. Issuing sanctions became a very real possibility in August 2015 when the Obama Administration released unprecedented targeted sanctions against specific Chinese companies and individuals who had benefitted from state stolen secrets. The sanctions served a dual purpose, first because they sent “a signal to Beijing that the administration is going to start fighting back on economic espionage,” and second because “it [sent] a signal to the private sector that we’re on your team. It tells China, enough is enough.”

If the threat of sanctions was the sole mechanism responsible for a marked decline in Chinese CE, then noticeable decreases in network intrusions following April and August 2015 would be expected and one finds this trend in Figure 5. From April to May 2015, there were approximately two less observed intrusions into American networks and from August to September 2015 there was a decrease in intrusions by about five. These immediate impacts seem to indicate that the threat of sanctions against Chinese companies and individuals played a role and had an impact on decreasing CE directed by the Chinese state.

---

Parity in Research and Development

My third proposed hypothesis for the decline in Chinese CE is that the leaders of the Chinese cyber apparatus no longer felt that they were gaining a competitive advantage by stealing research and development secrets from the United States. Instead, they might have felt that they had closed the previously existing gap and were now on par in production with the leading advanced economies of the world.

The United States remains the world’s leading entity in terms of gross total investment into research and development. However, China recently surpassed the United States in advanced late-stage research, the part of the inventive process that takes discoveries and turns them into profitable commercial products.157 What this trend indicates is that the United States invests substantial capital into the tedious work of developing new ideas, while China then takes those ideas and simply converts them into products to be sold on the market. As Corera states, certain designs “might have taken years of work and cost millions in research, but all the work could be siphoned off in a few moments.”158 This constant barrage of theft by China resulted in many advanced technologies being picked up in fairly developed stages and caused National Security Agency Director General Keith Alexander to complain that it constituted the greatest transfer of wealth in history.159

---

158 Corera, 193.
Figure 6 shows that Chinese-American investment in late-stage processes converged in 2013 and that by the end of 2018 Chinese investment in this area could double that of the United States if an aggressive growth rate is maintained.

The results of the trends reflected above are potentially troubling for American research entities because they invest billions into early-stage research and then do not reap the benefits of this process because competitors in the final stage take over. However, it is important to keep in mind that no other world actor can keep pace with the United States’ initial research and development capability. China specifically continues to rely on the United States and this is seen

---

through the doctrine of indigenous innovation. China relies on early United States research and this demonstrates a degree of interdependence between the two countries’ economies.

Through indigenous innovation, China employs a four-step process known as introduction, digestion, assimilation, and re-innovation. This central goal constitutes “the building of a sophisticated apparatus that brings in foreign technology and allows for the effective absorption and re-innovation of products that China can effectively claim to be homegrown.”\[^{161}\] China first obtains a technology it seeks to release into its domestic economic infrastructure and introduces it to the Chinese research and development community. It then allows the scientific community to analyze and understand the product. Next it aligns the introduced product with one that can be produced in China. Last the product is re-introduced as being originally created in China and late-stage development investment pays off because early money was saved on strenuous exploratory research. The Mandiant APT1 report shows that China possesses a honed ability to conduct acquisitive cyber operations and that through these capabilities it has “stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.”\[^{162}\] Fred Kaplan further describes this massive operation, noting that China targeted “defense contractors, waterworks, oil and gas pipelines, and other critical infrastructures. On average, these hackers lingered inside a targeted network for a full year.”\[^{163}\]

The one potential setback indigenous innovation poses to China is that it may not necessarily possess the domestic infrastructure or capability necessary to effectively make use of

\[^{161}\] Cheung, Lindsay, and Reveron, 66.
\[^{162}\] “APT1: Exposing One of China's Cyber Espionage Units.” Mandiant. 2004. \[https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf\]
\[^{163}\] Kaplan, 223.
all the technology it steals once they acquire it. Stephen Biddle argues that the information revolution experienced in the 20th and 21st centuries still poses problems for inquisitive and exploitative nations for three reasons: while more information is available than previously, it still is not perfect and likely will not be anytime soon, ambiguities in the information give rise to distortions that can lead to error in analysis, and because there is so much information available to be consumed, there is simply no way to effectively exploit all of the intelligence that is gathered. Moreover, Keohane and Nye agree with Biddle on this point in what they call the paradox of plenty. This paradox posits that the “low cost of transmitting data means that the ability to transmit it is much less important as a power resource than it used to be, but the ability to filter information is more so. Political struggles focus less on control over the ability to transmit information than over the creation and destruction of credibility.” This problem is also known as the wheat versus chaff predicament. The sheer volume of information coming in poses a problem for analysis, but there is also the “much more important matter of seeing this mass of material in its entirety, of being able to perceive patterns from day to day and reports that are anomalous.” If organizations are not capable of effectively absorbing, analyzing, and acting upon acquired information, then their collections efforts are useless.

It is not likely that China reached a point where the faith in its own domestic research and development capability allowed it to scale back its level of CE against the United States. America continues to be the world leader in early stage exploratory research and if China continues to invest heavily in late-stage development, it will need American products to work off

---

165 Keohane and Nye, 219.
of. Furthermore, because China began to outpace the United States in late-stage development investment as early as 2013 and FireEye’s report did not detect a significant decrease in Chinese CE incidents beginning until mid-2014, it is not likely that this hypothesis serves as a causal mechanism in understanding why Chinese CE habits changed.167

*Change in Political and Military Strategies*

My fourth proposed hypothesis observes that possible changes in Chinese political and military doctrines precipitated the change in CE tactics, and the FireEye Red Line Drawn report lends credence to this explanation. Chinese President Xi Jinping started a transformation of Chinese political and military doctrines early in 2013 following his election. All changes to these fields are in pursuit of protecting the longevity of the ruling Chinese Communist Party. This entails ensuring “domestic stability, territorial integrity, modernization, and economic growth, while simultaneously preparing for the possibility of militarized cyber conflict in the future.”168 To produce a force capable of fighting a cyber conflict, China’s *Science of Military Strategy* discusses the creation of elite, specialized network warfare forces.169 President Xi came to power at a time when Chinese leadership was riddled with corruption, it was viewed as being a minor power on the world stage, and its economic growth was slowing down as a result of domestic complications. To reverse this and implement his reforms, President Xi set about “consolidating

---

167 FireEye, Red Line Drawn.
personal power by creating new institutions, silencing political opposition, and legitimizing his leadership and the Communist Party’s power in the eyes of the Chinese people.”

The primary principled reform imposed by President Xi relating to cybersecurity was the consolidation and creation of the Cybersecurity and Informatization Leading Group in 2014. This body was formed by combining the previously existing State Informatization Leading Group and the State Network and Information Security Coordination Group. As Figure 1 shows, this new group reports directly to the Chinese Communist Party and is chaired by President Xi. The Cybersecurity and Informatization Leading Group’s role is to maintain “a multilevel protection scheme for critical infrastructure, cryptography for trusted systems, information security monitoring systems, crisis management processes, support for research and development in security, definition of technical standards, expanded professional education, and guaranteed funding for implementation.” As the supreme body on cybersecurity in China, this group plays a critical role in establishing what targets the Chinese cyber organization will go after and what methods will be employed. Its creation and the effect is has on the observed reduction of Chinese CE is manifested through the increased coordination in cyber activity brought about by a reduction in the number of government and military organizations pulling in opposing directions for cyber resources, the explicit combination of CE with military initiatives, and a reduction in the use of official state resources for criminal or other unauthorized purposes. Moreover, the Cybersecurity and Informatization Leading Group’s creation in 2014 coincides with the beginning of the reduction in detected Chinese intrusions into American corporations, thus

---

171 Cheung, Lindsay, and Reveron, 8.
suggesting that a reorientation of Chinese political and military strategy played a role in reduced CE.

Fulfillment of Summit Pledges

My fifth and final proposed explanation for reduced Chinese CE is that Presidents Obama and Xi both advised their respective organizations to adhere to the requirements outlined at their 2015 cybersecurity summit to cease CE against one another. At this September 2015 meeting, both governments agreed “that neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.”173 In order to accomplish this ambitious goal, the countries committed to increasing timely cooperation in the case of investigating malicious cyber-attacks originating from either country, they pledged to identify common efforts and work together to establish norms and accepted operating behavior for global cyber actors, and they promised to establish a high-level joint dialogue mechanism to help reduce cybercrime.174 Since the issuance of this joint proclamation, FireEye reports that “13 suspected China-based groups have compromised corporate networks in the U.S., Europe, and Japan, and targeted government, military, and commercial entities in the countries surrounding China.”175 While this indicates that China has not completely stopped its industrial espionage efforts against the United States, it has definitely dramatically reduced the scale at which and frequency with which it does so compared to pre-2014 levels.

---

174 Ibid.
Finally, Figure 5 indicates that the most noticeable and dramatic drop in Chinese CE occurred from August 2015 to September 2015. Because China was preparing for a United States state visit and knew that cybersecurity issues would be on the agenda, it is likely that it mandated its CE units to decrease attacks against the United States in order to reduce tension leading up to the summit. Lastly, it appears that this cybersecurity meeting, while not the beginning of the decline, played a major role in dramatically reducing Chinese CE intrusions to its current low levels by bringing attention to the issue and robbing China of its plausible deniability for its covert cyber operations.

It is impossible to know with complete certainty what caused a decline in Chinese CE beginning in mid-2014 without having access to classified high-level Chinese official communications and documents. However, the above analysis provides insight and several plausible junctures and events which helped to create a change in the way China steals secrets through cyberspace. First, indictments levied by the United States Department of Justice and the threat of sanctions against Chinese companies and individuals seem to both have played a role in causing a change of course. Second, a reorganization of Chinese cybersecurity decision-making power into the Cybersecurity and Informatization Leading Group seems to have cut down on duplication of efforts and served as an impetus for the state to more accurately direct efforts for CE. Lastly, the September 2015 summit between Presidents Obama and Xi seems to have caused a significant decline in Chinese CE as it brought their activities into the international spotlight.

The above reasons all likely had an additive and supplemental role in determining whether China would continue its CE operations at the breakneck pace with which they began and need not be mutually exclusive. However, there very well could be other explanations for the decreased numbers of intrusions detected by FireEye. For instance, China could have
intentionally planned to scale back its spying activity from a quantitative standpoint and instead decided to go after fewer, higher interest targets. Going further, Chinese CE hacking units could have adapted and made their methods and actions more covert so that they could no longer be detected. When considering explanations for the observed trend, what is most important is to avoid conflating American goals with Chinese goals and to realize that the two countries’ intentions almost certainly do not align. Avoiding mirror imaging, or assuming “that other leaders, states, and groups share motivations or goals similar to those most familiar” to the observer is important because it forces one to consider the relevant circumstances. Instead, political, economic, military, and cultural contexts must all be considered in order to isolate and make known what the most likely cause for the decrease appears to be.

Conclusions

The Chinese-United States bilateral relationship is likely the most important in the world. The two countries possess the two largest economies in the world, they boast two of the most formidable militaries in the entire world’s history, have powerful domestic political structures which also carry considerable clout in international governance organizations, and retain significant cultural influence with their traditions and cultures. With all of these similarities, China and the United States appear to interact in an interdependent relationship with one another by Keohane and Nye’s standard.

China and the United States have developed their complex interdependent relationship over the course of many decades; it was not the product of an overnight change in the policies of either side. Because this relationship is established and enduring, it is not likely that a change in its circumstances led to the rapid decline of Chinese CE against the United States in mid-2014.

176 Lowenthal, 162.
Instead, a combination of indictments levied by the United States Justice Department against five members of the People’s Liberation Army, the threat of sanctions against Chinese individuals and organizations, the creation and consolidation of Chinese cyber actors under the Cybersecurity and Informatization Leading Group, and the September 2015 summit between Presidents Obama and Xi all played a role in slowing Chinese spying.

When the United States displayed the will to enact penalties against Chinese organizations and individuals, it demonstrated that the United States was willing to change the shadow of the future and alter the direction of the Sino-American relationship. In a simple example, China was willing to settle for a 100% success rate in acquiring some of what they wanted and maintaining a predictable relationship with the United States rather than having a 95% success rate for everything they wanted that solicited an adverse response from the United States.

While the above trend has held true since the decline in Chinese CE, recent events and actions taken by the governments in Washington and Beijing might prove to affect the nature of Sino-American complex interdependence in the future. In March 2018, the Trump administration proposed $60 billion in tariffs on Chinese made steel and aluminum. In response, China announced that it plans to impose $3 billion in tariffs on American made fruit, pork, wine, seamless steel pipes and more than 100 other American made goods. The possible ensuing trade war could necessitate a dynamic change in the sensitivity and vulnerability factors of the Chinese-United States relationship. Moreover, the imposition of $60 billion in import taxes relegates Chinese products to a lower rung on the ladder than in the past. With their own

---

products now being at a distinct disadvantage, China might be more willing to take the added risk of trying to get everything they desire from the United States even if it means longer chances of success. Such actions could lead to renewed and increased CE to attain American intellectual property and business practices and decrease the level of complex interdependence between the two countries going forward.

Some in the United States have compared Chinese CE to piracy of centuries past and hope that as plundering others’ cargo was eventually deemed unacceptable, so too will China put an end to its theft of intellectual property. While the current levels of stealing seem to be moving in that direction, more work is clearly in store as international pressure and domestic control need to continue to force a total cessation of this activity.¹⁷⁸ Not all of the stated facets of complex interdependence theory can be readily identified in the Chinese-American relationship, but this does not mean that the two countries are not interdependent. Instead, what this shows is that Keohane and Nye’s model of complex interdependence is indeed an ideal type and the United States-Chinese relationship is a valid demonstration of their theory in practice in the real world. China and the United States are in a complex interdependent relationship in the meaningful sense of the term.¹⁷⁹

Cyber power and CE are different from traditional forms of state power for two primary reasons. First, the sheer volume of information that can be acquired through cyberspace is astronomical compared to traditional collection methods. Estimates of the amount of data stored by Amazon, Facebook, Google, and Microsoft assess that more than 1,200 petabytes are shared

¹⁷⁸ Corera, 200.
between the four.\textsuperscript{180} This figure excludes servers held in other countries and databases possessed by other major private companies in the United States, demonstrating just how overwhelming this flood of information is.

The second difference between actions in cyberspace and actions in the traditional real world are the blurred lines that now exist between military and civilian actors in cyberspace. For example, the United States Cyber Command and National Security Agency are both commanded by the same individual.\textsuperscript{181} This presents countries like the United States with unique challenges because military and civilian organizations operate under separate legal directives, so this combination could lead to a confusion of responsibilities. The unclear distinction between military and civilian actors along with the nature of cyberspace also makes attribution of actions more difficult. Managing the large amount of data being created every day will increasingly prove to be a viable indicator of a state’s ability to manage its interests in cyberspace effectively. Furthermore, handling the cultural differences between perceptions of national security and the legal distinctions found in some countries between military and civilian organizations will also prove to be important.

This case study examining complex interdependence between China and the United States holds broad implications for complex interdependence theory because it shows the increasing importance of multiple channels of communication and the growing significance of sensitivities and vulnerabilities in the information age. The rise of the Internet brought about with it the opportunity for individuals to connect with one another in a way that time and

\begin{itemize}
\end{itemize}
geography used to restrict.\textsuperscript{182} Because of these increasing connections, transnational and international groups have developed strategies for political bargaining that complex interdependence theory accounts for and predicts. This is especially true for China and the United States based on the high number of travelers the two countries exchange every year.

Second, sensitivity and vulnerability are core concepts in complex interdependence theory. With the rise of cyberspace, anonymity brought about concerns that it would be difficult to identify intrusions into one’s own networks and would thus bring about new challenges and costly effects that did not have to be previously accounted for. However, based on the interactions demonstrated between China and the United States starting with the indictment of five Chinese military hackers, we see that traditional avenues posited by complex interdependence theory, like interstate communication, are still leveraged in order to achieve favorable outcomes for both side’s goals. This in turn bolsters the case that absolute gains can be achieved in modern day complex interdependent relationships, and that these relationships should not just be considered in realist relative gains terms.

\textbf{Summary}

The three core tenets of complex interdependence hold that there must be multiple channels of communication between societies, there must be an absence of a hierarchy of issues, and there must not be a prevalence of military force used between the two actors. The United States and China currently demonstrate the characteristics of Keohane and Nye’s theory of complex interdependence but if the two countries’ interests further diverge in the future, a change in their interactions could occur.

\textsuperscript{182} Keohane and Nye, 194.
There are currently multiple channels of communication between China and the United States. First, there is interstate communication. This level of dialogue entails heads of state and other cabinet-level officials talking with one another in order to conduct official state business. Second, transgovernmental communication also exists and it is conversation carried out by non-governmental persons. Third, transnational communication is also conducted by organizations with global reach.

Just as there are multiple channels of communication, so too is there an absence of a hierarchy of issues. China and the United States deal with the lack of a common enemy, a large trade deficit, tensions over territory claims in the East and South China Seas, and animosity over how to handle circumstances surrounding Taiwan and North Korea.

Lastly, whether or not the criterion for lack of military conflict is met is up for debate. While there have not been outright conventional attacks between the two countries, China is developing its military capability and has also carried out actions in cyberspace that could be considered battlefield preparation. However, absent the prevalence of conventional military conflict between the two countries, it seems this condition is met.

Keohane and Nye also claim that four political conditions must be present in order for complex interdependence to exist: linkage strategies, agenda setting, transnational and transgovernmental relations, and the role played by international organizations. First, it seems that China is able to successfully create linkage strategies. Due to China’s frenetic pace of economic growth, it quickly consumed all of its domestic resources. As the economic pace of production slightly slowed, China transferred avenues of national pride into its revamped military. By building bases and ports around the world and tapping into Africa’s resource market, China was able to successfully create a linkage strategy.
Second, China also successfully sets its own agenda. By fulfilling its One Belt, One Road project, China prioritizes its own development over that of the nations it is extracting resources from. Additionally, China has a proven track record of disregarding international court rulings dealing with the East and South China Seas when the decision does not align with its interests.

Third, China and the United States do not meet the transnational and transgovernmental relations requirement. China allows its government and business elite to communicate with counterparts in the United States but they are not able to influence the domestic agenda in turn. Further, China closely monitors all of its citizens through Green Dam and the Great Firewall of China.

Lastly, international organizations do play a role in the China-United States relationship. For instance, environmental groups have worked hand-in-hand with the Chinese government to reduce coal consumption and carbon emissions in order to transition toward cleaner energy sources. Also, human rights groups based in the United States have closely monitored China’s Communist Party activities and recorded whenever abuses have occurred.

To conclude the interdependence section, power, sensitivity, and vulnerability are discussed. China exerts a tremendous amount of power and influence in cyberspace, with Operation Aurora as an example. In this program, China hacked Google and a number of other companies in order to observe dissidents and collect other information, like Google’s closely guarded source code. Moreover, the United States is sensitive in its relationship to China as the People’s Republic is America’s largest creditor and the United States runs a trade deficit over $300 billion with China. Lastly, the United States is also vulnerable to China, as events surrounding its interactions with North Korea over the past year show.
After discussing the intricacies of complex interdependence, this paper also investigated what caused Chinese CE to decline in mid-2014. Five possible causal mechanisms were proposed: the issuance of indictments by the United States Department of Justice against five People’s Liberation Army hackers, the threat of sanctions issued by the Obama administration in 2015, the fact that China’s government decided they no longer lagged behind the United States in terms of economic development so they no longer needed to steal, the reorganization and consolidation of Chinese military and political assets, and the September 2015 summit between Presidents Obama and Xi achieving the desired effects it set out to accomplish.

Of the above five possible explanations, it seems plausible and likely that the indictment of hackers, the threat of sanctions, the creation of the Cybersecurity and Informatization Leading Group, and the lead-up to the 2015 conference all played a significant role in causing the decline in China’s cyber spying. However, other causes cannot be totally ruled out as China may have just made their methods more covert or reorganized for increased efforts elsewhere.

With China burgeoning to take on an increased leadership role on the international stage, continued attention will be placed on its actions in cyberspace to make sure they are in accordance with international norms. As long as the United States desires to maintain its hegemonic position, it will continue to keep pressure on China’s cyber structure to ensure the integrity of its intellectual property and business plans system. The possible trade war between China and the United States could affect the degree of complex interdependence moving forward and provides an intriguing lead for future research.
Works Cited


